EXHIBIT C-7
EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(C)

Claim 6 ('661 Patent)	**U.S. 5,477,039 to Lisimaque et al. ("Lisimaque")**
A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	1:10-20 – "The present invention relates to a method and device to increase the protection of a chip or memory card. It is especially applicable to the making of microcircuit-based cards known as chip cards, used chiefly in fields where access to information or to services is strictly controlled. These are, in particular, credit cards in the field of banking, electronic badges used for subscriber television and for the distribution of gasoline and fuel, electronic cards providing access to the telephone system or again electronic cards providing access to certain data banks." 1:32-37 – "In the non-volatile memory there are also stored, firstly, the secret code identifying the bearer of the card with, if necessary, a ciphering program for the obtaining of a signature computed on the basis of the secret code and, secondly, instructions of the application program itself." 3:15-22 – "In this way, as can be seen in the diagram of FIG. 2, whenever a data element or command is sent to the card, the card can emit an end-of-control or acknowledgment signal CR acknowledging receipt of the data and commands that it has received after a period of time T. The duration of this time T, which is always random, can never provide information on the particular type of function that the card has been made to perform." 4:10-17 – "It must be noted that, in the cases of use of EPROM type non-volatile data memories, the above-described mechanisms for the generation of random numbers should be put into operation before any operation for the writing or erasure of these memories, for the fact of writing in these memories may cause variation in the voltage and/or the intensity of the supply current in a manner that is sufficiently significant to provide references for time measurements." 1:10-15 – "The present invention relates to a method and device to increase the protection of a chip or memory card. It is especially applicable to the making of microcircuit-based cards known as chip cards, used chiefly in fields where access to information or to services is strictly controlled."

	See also Scott Guthery, "Smart Cards," May 28, 1998, www.usenix.org/publications/login/1998-5/guthery.html (visited Dec. 5, 2006) (describing single-chip smart card processors as commonplace in the industry).
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:10-11 – "The present invention relates to a method and device to increase the protection of a chip or memory card." 1:22-26 – "In its broadest definition, a memory card has a storage device and a processing element formed by a microprocessor or any equivalent device, coupled to each other by a data and/or address bus that also connects the microcircuit thus formed to writing and reading devices external to the card." 1:47-50 & 62-65 – "[T]he user is generally allowed to make only a limited number of attempts to use his secret code in order to obtain access, with his card, to the services or information that he is seeking . . . . After each tabulation of a secret code, permission to have access to a service requested by a card-holder is generally given after the reception of an end-of-control message which is issued by the card after a ratification procedure, within a predetermined time limit following each attempt." 2:32-37 – "To this effect, an object of the invention is to provide a method to increase the protection of a microcircuit-based memory card comprising at least one memory coupled to a data-processing element wherein, when said data-processing element receives a command by a data signal external to the card . . . ." 2:67-3: -- "At step 1 data or commands are received by the microcircuit of the memory card." Claim 1 – "A memory card, said memory card comprising: a bus, said bus permitting communication between an external device and said memory card . . . ." Claim 5 – "A method to increase the security of a micro-circuit based chip card having a memory, and a data processing element receiving a data signal command from an external device ...." Figures 1, 3.
(b) a source of unpredictable information;	3:1-3 – "At steps 2 and 3 respectively, a random number A is drawn and pulses given continuously by a fixed clock (not shown) are counted in known way." 3:19-22 – "The duration of this time T, which is always random, can never provide information on the particular type of function that the

	card has been made to perform." Claim 1 – "A memory card, said memory card comprising: a bus, said bus permitting communication between an external device and said memory card; a first memory, said first memory being coupled to said bus, and said first memory having an application program stored therein; a second memory, said second memory being coupled to said bus; a circuit for generating a random delay value, said circuit being coupled to said bus; and a processing element, said processing element being coupled to said bus, and said processing element defining means for receiving instructions from said application program via said bus, for executing said application program instructions, for transmitting data via said bus to said second memory for storage therein, for receiving said random delay value via said bus, and for delaying transmission of an end-of-control signal from said memory card to said external device by an amount of time proportional to said random delay value." Claim 2 – "The memory card as in claim 1, wherein said random number circuit further comprises: a random code generator, said random code generator including a shift register, said shift register having inputs and outputs, and said shift register being controlled by a clock signal, and a plurality of exclusive-OR circuits, said exclusive-OR circuits connecting said outputs of said shift register to said inputs of said shift register; and a buffer register, said buffer register connecting said random code generator to said bus."
(c) a processor:	1:22-44 – "In its broadest definition, a memory card has a storage device and a processing element formed by a microprocessor or any equivalent device, coupled to each other by a data and/or address bus that also connects the microcircuit thus formed to writing and reading devices external to the card. The storage device generally includes a ROM or EPROM type non-volatile memory in which microprograms needed for the working of the processing element are recorded and, as the case may be, it includes a RAM type volatile memory for the memorizing of the data and the instructions specific to the application reserved to the memory card. In the non-volatile memory there are also stored, firstly, the secret code identifying the bearer of the card with, if necessary, a ciphering program for the obtaining of a signature computed on the basis of the secret code and, secondly, instructions of the application program itself. This signature is itself loaded into the volatile memory. Since the card has, firstly, the application program and, secondly, a ciphering algorithm identical to the one with which the signature has been prepared, it is enough, at each use, to ascertain that the new computation of the signature, on the basis of the instructions of the program and of the secret code, is truly equal to the

	signature that has been already recorded." 2:32-37 – "To this effect, an object of the invention is to provide a method to increase the protection of a microcircuit-based memory card comprising at least one memory coupled to a data-processing element wherein, when said data-processing element receives a command by a data signal external to the card . . . ." Claim 1: -- "a processing element."
(i) connected to said input interface for receiving and cryptographically processing said quantity,	1:22-44 – "In its broadest definition, a memory card has a storage device and a processing element formed by a microprocessor or any equivalent device, coupled to each other by a data and/or address bus that also connects the microcircuit thus formed to writing and reading devices external to the card. The storage device generally includes a ROM or EPROM type non-volatile memory in which microprograms needed for the working of the processing element are recorded and, as the case may be, it includes a RAM type volatile memory for the memorizing of the data and the instructions specific to the application reserved to the memory card. In the non-volatile memory there are also stored, firstly, the secret code identifying the bearer of the card with, if necessary, a ciphering program for the obtaining of a signature computed on the basis of the secret code and, secondly, instructions of the application program itself. This signature is itself loaded into the volatile memory. Since the card has, firstly, the application program and, secondly, a ciphering algorithm identical to the one with which the signature has been prepared, it is enough, at each use, to ascertain that the new computation of the signature, on the basis of the instructions of the program and of the secret code, is truly equal to the signature that has been already recorded." 2:32-37 – "To this effect, an object of the invention is to provide a method to increase the protection of a microcircuit-based memory card comprising at least one memory coupled to a data-processing element wherein, when said data-processing element receives a command by a data signal external to the card . . . ."
(ii) configured to use said unpredictable information to conceal a correlation between said microchip's power consumption and said processing of said quantity by	3:1-13 – "At steps 2 and 3 respectively, a random number A is drawn and pulses given continuously by a fixed clock (not shown) are counted in known way. Simultaneously, a program corresponding to the data and/or to the corresponding command is launched at step 4 to carry out operations for writing, reading the memory of the card and/or for example computing a signature. At the end of the execution of these instructions, the program emits an end-of-control signal or acknowledgment signal at step 5. At step 6, a comparison is made between the random number drawn at step 2 and the count made at step 3. When the number indicated by the count at step 3 is equal to the

expending additional electricity in said microchip during said processing; and	random number obtained at step 6, the end-of-control signal emitted at step 5 is validated at step 7." 4:10-17 - "It must be noted that, in the cases of use of EPROM type non-volatile data memories, the above-described mechanisms for the generation of random numbers should be put into operation before any operation for the writing or erasure of these memories, for the fact of writing in these memories may cause variation in the voltage and/or the intensity of the supply current in a manner that is sufficiently significant to provide references for time measurements." 3:15-22 – "In this way, as can be seen in the diagram of FIG. 2, whenever a data element or command is sent to the card, the card can emit an end-of-control or acknowledgment signal CR acknowledging receipt of the data and commands that it has received after a period of time T. The duration of this time T, which is always random, can never provide information on the particular type of function that the card has been made to perform."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	1:22-26 – "In its broadest definition, a memory card has a storage device and a processing element formed by a microprocessor or any equivalent device, coupled to each other by a data and/or address bus that also connects the microcircuit thus formed to writing and reading devices external to the card." 3:3-6 & 13-15 – "Simultaneously, a program corresponding to the data and/or to the corresponding command is launched at step 4 to carry out operations for writing, reading the memory of the card and/or for example computing a signature. At the end of the execution of these instructions, the program emits an end-of-control signal or acknowledgment signal at step 5 . . . . Then, at step 8, this signal is sent out of the card into a card reading/writing device (not shown)." Figure 1.

Claim 7 ('661 Patent)	**U.S. 5,477,039 to Lisimaque**
The device of claim 6 including program logic to activate said expending during said processing.	3:38-46 – "An embodiment of a circuit 19 for the implementation of the above method and its interconnection with the elements forming a memory card are shown in FIG. 4. The circuit 19 has a random code generator shown within a box of dashed lines 10. The parallel outputs of the generator 10 are connected to the parallel inputs of a buffer register 11. In the example of FIG. 4, the random code generator has, in a known way, a shift register 12 with outputs looped to inputs

	through exclusive-OR circuits 130, 140." 3:54-66 – "To execute the method according to the invention, the shift register 12 is preferably controlled at the rate of a clock signal CK which is different from the clock signal used to determine the processing cycles of the processing unit 16. When, as shown in FIG. 3, the processing unit 16 carries out the control program 4 to draw the random number A, a reading signal UT of the processing unit 16 is applied to a control input of the buffer register 11 to hold the drawn random number A in the register and provide for its transfer to the bus 13. It must be noted that, according to this approach, the clock signal CK may be made variable, notably as a function of the temperature and of the supply voltages of the card so as to also have a random character." Claim 1 – "A memory card, said memory card comprising: a bus, said bus permitting communication between an external device and said memory card; a first memory, said first memory being coupled to said bus, and said first memory having an application program stored therein; a second memory, said second memory being coupled to said bus; a circuit for generating a random delay value, said circuit being coupled to said bus; and a processing element, said processing element being coupled to said bus, and said processing element defining means for receiving instructions from said application program via said bus, for executing said application program instructions, for transmitting data via said bus to said second memory for storage therein, for receiving said random delay value via said bus, and for delaying transmission of an end-of-control signal from said memory card to said external device by an amount of time proportional to said random delay value." Claim 2 – "The memory card as in claim 1, wherein said random number circuit further comprises: a random code generator, said random code generator including a shift register, said shift register having inputs and outputs, and said shift register being controlled by a clock signal, and a plurality of exclusive-OR circuits, said exclusive-OR circuits connecting said outputs of said shift register to said inputs of said shift register; and a buffer register, said buffer register connecting said random code generator to said bus." Figure 4.

Claim 8 ('661 Patent)	**U.S. 5,477,039 to Lisimaque**
The device of claim 7	3:38-46 – "An embodiment of a circuit 19 for the implementation of

including (a) program logic implementing said source of unpredictable information; and	the above method and its interconnection with the elements forming a memory card are shown in FIG. 4. The circuit 19 has a random code generator shown within a box of dashed lines 10. The parallel outputs of the generator 10 are connected to the parallel inputs of a buffer register 11. In the example of FIG. 4, the random code generator has, in a known way, a shift register 12 with outputs looped to inputs through exclusive-OR circuits 130, 140." Claim 1 – "A memory card, said memory card comprising: a bus, said bus permitting communication between an external device and said memory card; a first memory, said first memory being coupled to said bus, and said first memory having an application program stored therein; a second memory, said second memory being coupled to said bus; a circuit for generating a random delay value, said circuit being coupled to said bus; and a processing element, said processing element being coupled to said bus, and said processing element defining means for receiving instructions from said application program via said bus, for executing said application program instructions, for transmitting data via said bus to said second memory for storage therein, for receiving said random delay value via said bus, and for delaying transmission of an end-of-control signal from said memory card to said external device by an amount of time proportional to said random delay value." Claim 2 – "The memory card as in claim 1, wherein said random number circuit further comprises: a random code generator, said random code generator including a shift register, said shift register having inputs and outputs, and said shift register being controlled by a clock signal, and a plurality of exclusive-OR circuits, said exclusive-OR circuits connecting said outputs of said shift register to said inputs of said shift register; and a buffer register, said buffer register connecting said random code generator to said bus." Figure 4.
(b) program logic to transmit said unpredictable information to an additional power expending circuit contained in said microchip.	3:38-46 – "An embodiment of a circuit 19 for the implementation of the above method and its interconnection with the elements forming a memory card are shown in FIG. 4. The circuit 19 has a random code generator shown within a box of dashed lines 10. The parallel outputs of the generator 10 are connected to the parallel inputs of a buffer register 11. In the example of FIG. 4, the random code generator has, in a known way, a shift register 12 with outputs looped to inputs through exclusive-OR circuits 130, 140." 3:54-66 – "To execute the method according to the invention, the shift register 12 is preferably controlled at the rate of a clock signal CK which is different from the clock signal used to determine the

	processing cycles of the processing unit 16. When, as shown in FIG. 3, the processing unit 16 carries out the control program 4 to draw the random number A, a reading signal UT of the processing unit 16 is applied to a control input of the buffer register 11 to hold the drawn random number A in the register and provide for its transfer to the bus 13. It must be noted that, according to this approach, the clock signal CK may be made variable, notably as a function of the temperature and of the supply voltages of the card so as to also have a random character." Claim 1 – "A memory card, said memory card comprising: a bus, said bus permitting communication between an external device and said memory card; a first memory, said first memory being coupled to said bus, and said first memory having an application program stored therein; a second memory, said second memory being coupled to said bus; a circuit for generating a random delay value, said circuit being coupled to said bus; and a processing element, said processing element being coupled to said bus, and said processing element defining means for receiving instructions from said application program via said bus, for executing said application program instructions, for transmitting data via said bus to said second memory for storage therein, for receiving said random delay value via said bus, and for delaying transmission of an end-of-control signal from said memory card to said external device by an amount of time proportional to said random delay value." Claim 2 – "The memory card as in claim 1, wherein said random number circuit further comprises: a random code generator, said random code generator including a shift register, said shift register having inputs and outputs, and said shift register being controlled by a clock signal, and a plurality of exclusive-OR circuits, said exclusive-OR circuits connecting said outputs of said shift register to said inputs of said shift register; and a buffer register, said buffer register connecting said random code generator to said bus." Figure 4.

Claim 11 ('661 Patent)	**U.S. 5,477,039 to Lisimaque**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to	1:10-20 – "The present invention relates to a method and device to increase the protection of a chip or memory card. It is especially applicable to the making of microcircuit-based cards known as chip cards, used chiefly in fields where access to information or to services is strictly controlled. These are, in particular, credit cards in the field of banking, electronic badges used for subscriber television and for

discovery of a secret by external measurement of said device's power consumption, comprising:	the distribution of gasoline and fuel, electronic cards providing access to the telephone system or again electronic cards providing access to certain data banks." 1:32-37 – "In the non-volatile memory there are also stored, firstly, the secret code identifying the bearer of the card with, if necessary, a ciphering program for the obtaining of a signature computed on the basis of the secret code and, secondly, instructions of the application program itself." 3:15-22 – "In this way, as can be seen in the diagram of FIG. 2, whenever a data element or command is sent to the card, the card can emit an end-of-control or acknowledgment signal CR acknowledging receipt of the data and commands that it has received after a period of time T. The duration of this time T, which is always random, can never provide information on the particular type of function that the card has been made to perform." 4:10-17 – "It must be noted that, in the cases of use of EPROM type non-volatile data memories, the above-described mechanisms for the generation of random numbers should be put into operation before any operation for the writing or erasure of these memories, for the fact of writing in these memories may cause variation in the voltage and/or the intensity of the supply current in a manner that is sufficiently significant to provide references for time measurements."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:10-11 – "The present invention relates to a method and device to increase the protection of a chip or memory card." 1:22-26 – "In its broadest definition, a memory card has a storage device and a processing element formed by a microprocessor or any equivalent device, coupled to each other by a data and/or address bus that also connects the microcircuit thus formed to writing and reading devices external to the card." 1:47-50 & 62-65 – "[T]he user is generally allowed to make only a limited number of attempts to use his secret code in order to obtain access, with his card, to the services or information that he is seeking . . . . After each tabulation of a secret code, permission to have access to a service requested by a card-holder is generally given after the reception of an end-of-control message which is issued by the card after a ratification procedure, within a predetermined time limit following each attempt." 2:32-37 – "To this effect, an object of the invention is to provide a method to increase the protection of a microcircuit-based memory card comprising at least one memory coupled to a data-processing

	element wherein, when said data-processing element receives a command by a data signal external to the card . . . ." 2:67-3: -- "At step 1 data or commands are received by the microcircuit of the memory card." Claim 1 – "A memory card, said memory card comprising: a bus, said bus permitting communication between an external device and said memory card . . . ." Claim 5 – "A method to increase the security of a micro-circuit based chip card having a memory, and a data processing element receiving a data signal command from an external device ...." Figures 1, 3.
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:22-26 – "In its broadest definition, a memory card has a storage device and a processing element formed by a microprocessor or any equivalent device, coupled to each other by a data and/or address bus that also connects the microcircuit thus formed to writing and reading devices external to the card." 2:32-37 – "To this effect, an object of the invention is to provide a method to increase the protection of a microcircuit-based memory card comprising at least one memory coupled to a data-processing element wherein, when said data-processing element receives a command by a data signal external to the card . . . ." 2:67-3: -- "At step 1 data or commands are received by the microcircuit of the memory card." 4:10-17 -- "It must be noted that, in the cases of use of EPROM type non-volatile data memories, the above-described mechanisms for the generation of random numbers should be put into operation before any operation for the writing or erasure of these memories, for the fact of writing in these memories may cause variation in the voltage and/or the intensity of the supply current in a manner that is sufficiently significant to provide references for time measurements." Claim 1 – "A memory card, said memory card comprising: a bus, said bus permitting communication between an external device and said memory card . . . ." Claim 5 – "A method to increase the security of a micro-circuit based chip card having a memory, and a data processing element receiving a data signal command from an external device ...." 3:63-66 – "It must be noted that, according to this approach, the clock

	signal CK may be made variable, notably as a function of the temperature and of the supply voltages of the card so as to also have a random character." 4:13-16 – "[T]he fact of writing in these memories may cause variation in the voltage and/or the intensity of the supply current in a manner that is sufficiently significant to provide references for time measurements." Figures 1, 3.
(c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and	1:22-44 – "In its broadest definition, a memory card has a storage device and a processing element formed by a microprocessor or any equivalent device, coupled to each other by a data and/or address bus that also connects the microcircuit thus formed to writing and reading devices external to the card. The storage device generally includes a ROM or EPROM type non-volatile memory in which microprograms needed for the working of the processing element are recorded and, as the case may be, it includes a RAM type volatile memory for the memorizing of the data and the instructions specific to the application reserved to the memory card. In the non-volatile memory there are also stored, firstly, the secret code identifying the bearer of the card with, if necessary, a ciphering program for the obtaining of a signature computed on the basis of the secret code and, secondly, instructions of the application program itself. This signature is itself loaded into the volatile memory. Since the card has, firstly, the application program and, secondly, a ciphering algorithm identical to the one with which the signature has been prepared, it is enough, at each use, to ascertain that the new computation of the signature, on the basis of the instructions of the program and of the secret code, is truly equal to the signature that has been already recorded." 2:32-37 – "To this effect, an object of the invention is to provide a method to increase the protection of a microcircuit-based memory card comprising at least one memory coupled to a data-processing element wherein, when said data-processing element receives a command by a data signal external to the card . . . ." Claim 1: -- "a processing element."
(d) a noise production system for introducing noise into said measurement of said power consumption.	2:2-7 -- "This operation thus leaves fraudulent persons, having sophisticated means, with the possibility of finding the secret codes by methodically trying out every possible code for example, and noting down the time taken by the card to emit the end-of-control message each time they present the card." Claim 1: -- "a processing element, said processing element being

	coupled to said bus, and said processing element defining means for receiving instructions from said application program via said bus, for executing said application program instructions, for transmitting data via said bus to said second memory for storage therein, for receiving said random delay value via said bus, and for delaying transmission of an end-of-control signal from said memory card to said external device by an amount of time proportional to said random delay value." Claim 2: – "wherein said random number circuit further comprises: a random code generator, said random code generator including a shift register, said shift register having inputs and outputs, and said shift register being controlled by a clock signal, and a plurality of exclusive-OR circuits, said exclusive-OR circuits connecting said outputs of said shift register to said inputs of said shift register; and a buffer register, said buffer register connecting said random code generator to said bus." Figure 4.

Claim 22 ('661 Patent)	**U.S. 5,477,039 to Lisimaque**
A device according to claims 1, 4, 7, 9, 11, 14, 15, or 20 wherein said device comprises a smartcard.	1:10-20 – "The present invention relates to a method and device to increase the protection of a chip or memory card. It is especially applicable to the making of microcircuit-based cards known as chip cards, used chiefly in fields where access to information or to services is strictly controlled. These are, in particular, credit cards in the field of banking, electronic badges used for subscriber television and for the distribution of gasoline and fuel, electronic cards providing access to the telephone system or again electronic cards providing access to certain data banks."

Claim 29 ('661 Patent)	**U.S. 5,477,039 to Lisimaque**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of	1:10-20 – "The present invention relates to a method and device to increase the protection of a chip or memory card. It is especially applicable to the making of microcircuit-based cards known as chip cards, used chiefly in fields where access to information or to services is strictly controlled. These are, in particular, credit cards in the field of banking, electronic badges used for subscriber television and for the distribution of gasoline and fuel, electronic cards providing access to the telephone system or again electronic cards providing access to

said device's power consumption, comprising:	certain data banks." 1:32-37 – "In the non-volatile memory there are also stored, firstly, the secret code identifying the bearer of the card with, if necessary, a ciphering program for the obtaining of a signature computed on the basis of the secret code and, secondly, instructions of the application program itself." 3:15-22 – "In this way, as can be seen in the diagram of FIG. 2, whenever a data element or command is sent to the card, the card can emit an end-of-control or acknowledgment signal CR acknowledging receipt of the data and commands that it has received after a period of time T. The duration of this time T, which is always random, can never provide information on the particular type of function that the card has been made to perform." 4:10-17 – "It must be noted that, in the cases of use of EPROM type non-volatile data memories, the above-described mechanisms for the generation of random numbers should be put into operation before any operation for the writing or erasure of these memories, for the fact of writing in these memories may cause variation in the voltage and/or the intensity of the supply current in a manner that is sufficiently significant to provide references for time measurements."
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	3:47-52 – "The connection of the circuit 19 to the other elements which, in a standard way, form a memory card, is done by means of the data bus 13 of these cards which connect RAM type memories 14 and ROM or EPROM type memories 15 to their processing unit 16. The connection to the data bus 13 takes place through the outputs of the buffer register 11." 3:63-66 – "It must be noted that, according to this approach, the clock signal CK may be made variable, notably as a function of the temperature and of the supply voltages of the card so as to also have a random character." 4:13-16 – "[T]he fact of writing in these memories may cause variation in the voltage and/or the intensity of the supply current in a manner that is sufficiently significant to provide references for time measurements." Figure 4.
(b) receiving a quantity to be cryptographically processed, said	1:10-11 – "The present invention relates to a method and device to increase the protection of a chip or memory card." 1:22-26 – "In its broadest definition, a memory card has a storage

quantity being representative of at least a portion of a message;	device and a processing element formed by a microprocessor or any equivalent device, coupled to each other by a data and/or address bus that also connects the microcircuit thus formed to writing and reading devices external to the card." 2:32-37 – "To this effect, an object of the invention is to provide a method to increase the protection of a microcircuit-based memory card comprising at least one memory coupled to a data-processing element wherein, when said data-processing element receives a command by a data signal external to the card . . . ." Claim 1 – "A memory card, said memory card comprising: a bus, said bus permitting communication between an external device and said memory card . . . ." Claim 5: -- "A method to increase the security of a micro-circuit based chip card having a memory, and a data processing element receiving a data signal command from an external device ...." Figures 1, 3.
(c) introducing noise into said measurement of said power consumption while processing said quantity; and	2:2-7 – "This operation thus leaves fraudulent persons, having sophisticated means, with the possibility of finding the secret codes by methodically trying out every possible code for example, and noting down the time taken by the card to emit the end-of-control message each time they present the card." Claim 1: -- "a processing element, said processing element being coupled to said bus, and said processing element defining means for receiving instructions from said application program via said bus, for executing said application program instructions, for transmitting data via said bus to said second memory for storage therein, for receiving said random delay value via said bus, and for delaying transmission of an end-of-control signal from said memory card to said external device by an amount of time proportional to said random delay value." Claim 2: -- "wherein said random number circuit further comprises: a random code generator, said random code generator including a shift register, said shift register having inputs and outputs, and said shift register being controlled by a clock signal, and a plurality of exclusive-OR circuits, said exclusive-OR circuits connecting said outputs of said shift register to said inputs of said shift register; and a buffer register, said buffer register connecting said random code generator to said bus." Figure 4.

(d) outputting said cryptographically processed quantity to a recipient thereof.	1:22-26 – "In its broadest definition, a memory card has a storage device and a processing element formed by a microprocessor or any equivalent device, coupled to each other by a data and/or address bus that also connects the microcircuit thus formed to writing and reading devices external to the card." 3:3-6 & 13-15 – "Simultaneously, a program corresponding to the data and/or to the corresponding command is launched at step 4 to carry out operations for writing, reading the memory of the card and/or for example computing a signature. At the end of the execution of these instructions, the program emits an end-of-control signal or acknowledgment signal at step 5 . . . . Then, at step 8, this signal is sent out of the card into a card reading/writing device (not shown)." Figure 1.